

07/21/00
JC490 U.S. PTO

07-24-00

A

PATENT
Docket No. PD-200045
CUSTOMER NO.: 020991

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
APPLICATION TRANSMITTAL LETTER FOR
NONPROVISIONAL PATENT APPLICATION
Under 37 C.F.R. 1.53(b)

JC857 U.S. PTO
09/620772
07/21/00


Certification under 37 CFR 1.10 (if applicable)

EL447059716US
EXPRESS MAIL mailing number

July 21, 2000
Date of Deposit

I hereby certify that this application is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, DC 20231.

Dana J. Warnquist
(Type or printed name of person mailing application)


(Signature of person mailing application)

Assistant Commissioner for Patents
Washington, DC 20231

Sir:
Transmitted herewith for filing is the patent application, including 5 sheets of formal/~~informal~~ drawings, of
inventors: **Raynold M. Kahn, Gregory J. Gagnon, David D. Ha, Peter M. Klauss, Christopher P. Curren, Thomas H. James**
for: **SUPER ENCRYPTED STORAGE AND RETRIEVAL OF MEDIA PROGRAMS WITH SMARTCARD GENERATED KEYS**

The filing fee for this application is calculated below:

	CLAIMS AS FILED			
	NUMBER FILED		NUMBER EXTRA	RATE
Basic Fee				\$ 0.00
Total Claims	42	-20 =	22 x	\$ 18.00
Independent Claims	3	- 3 =	0 x	\$ 78.00
Multiple Dependent Claims			+	\$260.00
TOTAL FILING FEE :				\$ 0.00

Please charge Deposit Account No. 50-0383 of Hughes Electronics Corporation, El Segundo, California, in the amount of **\$0.00**. The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment, to that account.

The Commissioner is further hereby authorized to charge to said above Deposit Account No. 50-0383, pursuant to 37 CFR 1.25(b), any fees whatsoever which may properly become due or payable, as set forth in 37 CFR 1.16 to 1.17 inclusive, for the entire pendency of this application without specific additional authorization.

Please associate this application with the Hughes Electronics Corporation Customer Number 020991.

This form is submitted in triplicate.


HUGHES ELECTRONICS CORPORATION
John A. Crook, Registration No.: 30,830
Attorney for Applicants

CUSTOMER NUMBER 020991
HUGHES ELECTRONICS CORPORATION
Bldg. 001, M/S A109
PO Box 956
El Segundo, CA 90245-0956
Telephone: 303/712.5044
Date: July 21, 2000

PATENT
PD-200045

SUPER ENCRYPTED STORAGE AND RETRIEVAL OF MEDIA PROGRAMS WITH
SMARTCARD GENERATED KEYS

Inventors:

Raynold M. Kahn
Gregory J. Gagnon
David D. Ha
Peter M. Klauss
Christopher P. Curren
Thomas H. James

SUPER ENCRYPTED STORAGE AND RETRIEVAL OF MEDIA PROGRAMS WITH
SMARTCARD GENERATED KEYS

CROSS-REFERENCE TO RELATED APPLICATIONS

5 This application is related to the following patent applications, all of which applications are hereby incorporated by reference herein:

U.S. Patent Application Serial No. --/---,---, entitled "SECURE STORAGE AND
REPLAY OF MEDIA PROGRAMS USING A HARD-PAIRED RECEIVER AND
STORAGE DEVICE," by Raynold M. Kahn, Gregory J. Gagnon, David D. Ha, Peter M.
10 Klauss, Christopher P. Curren, and Thomas H. James, attorney's docket number PD-
200042, filed on same date herewith;

U.S. Patent Application Serial No. --/---,---, entitled "SUPER ENCRYPTED
STORAGE AND RETRIEVAL OF MEDIA PROGRAMS IN A HARD-PAIRED
RECEIVER AND STORAGE DEVICE," by Raynold M. Kahn, Gregory J. Gagnon,
15 David D. Ha, Peter M. Klauss, Christopher P. Curren, and Thomas H. James, attorney's
docket number PD-200043, filed on same date herewith;

U.S. Patent Application Serial No. --/---,---, entitled "SUPER ENCRYPTED
STORAGE AND RETRIEVAL OF MEDIA PROGRAMS WITH MODIFIED
CONDITIONAL ACCESS FUNCTIONALITY," by Raynold M. Kahn, Gregory J.
20 Gagnon, David D. Ha, Peter M. Klauss, Christopher P. Curren, and Thomas H. James,
attorney's docket number PD-200044, filed on same date herewith;

U.S. Patent Application Serial No. --/---,---, entitled "VIDEO ON DEMAND
PAY PER VIEW SERVICES WITH UNMODIFIED CONDITIONAL ACCESS
FUNCTIONALITY" by Raynold M. Kahn, Gregory J. Gagnon, David D. Ha, Peter M.
25 Klauss, Christopher P. Curren, and Thomas H. James, attorney's docket number PD-
200055, filed on same date herewith; and

U.S. Patent Application Serial No. 09/491,959, entitled "VIRTUAL VIDEO ON
DEMAND USING MULTIPLE ENCRYPTED VIDEO SEGMENTS," by Robert G.
Arsenault and Leon J. Stanger, attorney's docket number PD-980208, filed on January 26,
30 2000.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to systems and methods for providing video program material to subscribers, and in particular to a method and system for securely storing and
5 replaying media programs.

2. Description of the Related Art

In recent years, there has been increasing interest in allowing cable and satellite television subscribers to record broadcast media programs for later viewing. This
10 capability, hereinafter referred to as personal video recording (PVR), can be used to provide video-on-demand (VOD) services, or simply to allow the subscriber to save media programs for repeated viewing and/or archival purposes.

In the past, video cassette tape recorders (VCRs) have been used for such personal video recording. Recently, however, hard disks, similar to those used in personal
15 computers, have been used to store media programs for later viewing. Unlike VCRs, such devices typically do not include a tuner, and are instead coupled to the satellite receiver or cable box. Also unlike VCRs, these devices are typically used to record digital content, not analog video. This difference is both advantageous and disadvantageous.

An advantage of such devices is that they permit long term storage and multiple
20 replays without substantial degradation. Another advantage is that they permit more rapid trick-play functions such as fast forwarding and rewinding. A disadvantage of such devices is that they are capable of making multiple-generation copies of the program material as well, and without serious degradation. This raises the very real possibility
25 that the multiple generation copies of the media programs will be produced and distributed without permission. This possibility has caused some media providers to be reluctant to allow their media programs to be recorded by such devices.

To ameliorate this problem, it is critical to protect the stored media programs with
strong security and copy control. Current devices do not scramble media programs before
30 storage, nor do they store copy protection information. Instead, such devices record decrypted program content into the storage disk using a paired hardware scheme in which

the hard disk controller and hard disk are paired to each other specifically through a specific interface. Because the hard disk controller and the disk itself are essentially paired together, storage or playback will not function if the disk were to be removed and transferred to another player. The weakness of this security scheme is that it relies only
5 on the paired hardware to ensure security ... the media programs stored on the disk drive itself are not encrypted.

While it would presumably be possible to simply store the datastream as it is received from the broadcaster for later replay, this technique has distinct disadvantages. One such disadvantage is that it would provide pirates a permanently recorded version of
10 the encrypted datastream, thus providing the pirate with information that can be used to perform detailed analyses of the datastream itself to determine the encryption techniques and codes.

What is needed is a system and method for securely recording broadcast media programs (including impulse purchase pay-per-view programs) for limited use playback
15 at a later time. Such a system could be used to support video-on-demand (VOD), thus allowing the subscriber to purchase media programs and games from the set top box instantly without worrying about the start time of the program. What is also needed is a system and method that does not require substantial changes to subscriber hardware, such as the integrated receiver/decoder (IRD), or the conditional access module (CAM) that is
20 used to provide a key to decrypt the media programs for presentation to the subscribers.

SUMMARY OF THE INVENTION

In summary, the present invention describes a system and method for storing and retrieving program material for subsequent replay. The method comprises the steps of
25 accepting encrypted access control information and the program material encrypted according to a first encryption key, the access control information including a first encryption key and control data; decrypting the received access control information to produce the first encryption key; decrypting the program material using the first encryption key; re-encrypting the program material according to a second encryption key;
30 encrypting the second encryption key according to a third encryption key to produce a

fourth encryption key; and providing the re-encrypted program material and a fourth encryption key for storage.

The apparatus comprises a conditional access module, for accepting encrypted access control information and the program material encrypted according to a first encryption key, the encrypted access control information including the first encryption key and temporally-variant control data, the control access module comprising a first decryption module, for decrypting the access control information to produce the first encryption key; a first encryption module for encrypting a second encryption key with a third encryption key to produce a fourth encryption key; and a second decryption module for decrypting the fourth encryption key to produce the second encryption key.

One object of the present invention is to provide for the reception and decryption of broadcast media programs, including impulse pay-per-view (IPPV) programs, that can be played and recorded onto storage media and allows playback at a later time with limited use. The data itself may be placed in short term storage, but the replay of the media programs can be accomplished with trick play functions such as forward, reverse, fast forward, fast reverse, frame advance, and pause functions.

Another object of the present invention is to provide PVR functions which provide recording, delayed playback, and trick play of IPPV media programs from the storage media without requiring a pre-purchase of the IPPV media program. This would allow the IPPV media program to be viewed without requiring the IPPV media program to be purchased prior to storage. Ideally, such a system would allow the user to select the IPPV media program from the storage device, subject to limited play rights.

Still another object of the present invention is to provide a pairing between the storage media and elements of the subscriber's IRD to assure that playback of the media programs from the storage device is permitted only with the proper IRD.

Still another object of the present invention is to provide a secure means for storing broadcast data streams (including IPPV and games) on a data storage device, while providing for adequate copy protection.

Still another object of the present invention is to provide a system and method for handling the archiving and retrieving of media programs and other data, even if the data storage device fails.

Still another object of the present invention is to provide a system and method that allows media program purchases to be recorded in a way that is analogous to that which is employed for real-time off-the-air programs.

5 Still another object of the present invention is to provide a system that provides a growth path to a system permitting IPPV media programs to be previewed without charge for an initial period of time with the option to purchase the media program or cancel the purchase, regardless of whether the program is retrieved from the storage device or obtained from a real time broadcast.

10 The present invention eliminates concerns regarding the proliferation of unauthorized digital copies of the media programs by use of a strong encryption method. Further, the present invention ensures that the stored material cannot be distributed since such decryption of the material can only be successfully performed by the encrypting IRD.

15 BRIEF DESCRIPTION OF THE DRAWINGS

Referring now to the drawings in which like reference numbers represent corresponding parts throughout:

FIG. 1 is a diagram showing an overview of a video distribution system;

20 FIG. 2 is a block diagram showing a typical uplink configuration showing how video program material is uplinked to a satellite for transmission to subscribers using a single transponder;

FIG. 3A is a diagram of a representative data stream received from a satellite;

FIG. 3B is a diagram illustrating the structure of a data packet;

FIG. 4 is a block diagram illustrating a high-level block diagram of the IRD; and

25 FIG. 5 is a diagram illustrating the storage and retrieval of data from a media storage device.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

30 In the following description, reference is made to the accompanying drawings which form a part hereof, and which show, by way of illustration, several embodiments of the present invention. It is understood that other embodiments may be utilized and

structural changes may be made without departing from the scope of the present invention.

VIDEO DISTRIBUTION SYSTEM

5 FIG. 1 is a diagram illustrating an overview of a video distribution system 100. The video distribution system 100 comprises a control center 102 in communication with an uplink center 104 via a ground link 114 and an integrated receiver/decoder (IRD) 132 at receiver station 130 via a public switched telephone network (PSTN) or other link 120. The control center 102 provides program material to the uplink center 104, coordinates
10 with the receiver station 130 to offer subscribers 110 pay-per-view (PPV) program services, including billing and associated decryption of video programs.

 The uplink center 104 receives program material and program control information from the control center 102, and using an uplink antenna 106, transmits the program material and program control information to the satellite 108. The satellite 108 receives
15 and processes this information, and transmits the video programs and control information to the IRD 132 at the receiver station 130 via downlink 118. The IRD 132 receives this information using the subscriber antenna 112 to which it is communicatively coupled.

 The video distribution system 100 can comprise a plurality of satellites 108 in order to provide wider terrestrial coverage, to provide additional channels, or to provide
20 additional bandwidth per channel. In one embodiment of the invention, each satellite comprises 16 transponders to receive and transmit program material and other control data from the uplink center 104 and provide it to the subscribers 110. However, using data compression and multiplexing techniques the channel capabilities are far greater. For example, two-satellites 108 working together can receive and broadcast over 150
25 conventional (non-HDTV) audio and video channels via 32 transponders.

 While the invention disclosed herein will be described with reference to a satellite based video distribution system 100, the present invention may also be practiced with terrestrial-based transmission of program information, whether by traditional
30 broadcasting means, cable, or other means. Further, the different functions collectively allocated among the control center 102 and the uplink center 104 as described above can

be reallocated as desired without departing from the intended scope of the present invention.

Although the foregoing has been described with respect to an embodiment in which the program material delivered to the subscriber is video (and audio) program material such as a movie, the foregoing method can be used to deliver program material comprising purely audio information or data as well.

FIG. 2 is a block diagram showing a typical uplink configuration for a single satellite 108 transponder, showing how video program material is uplinked to the satellite 108 by the control center 102 and the uplink center 104. FIG. 2 shows three video channels (which could be augmented respectively with one or more audio channels for high fidelity music, soundtrack information, or a secondary audio program for transmitting foreign languages), and a data channel from a computer data source 206.

The video channels are provided by a program source of video material 200A-200C (collectively referred to hereinafter as video source(s) 200). The data from each video program source 200 is provided to an encoder 202A-202C (collectively referred to hereinafter as encoder(s) 202). Each of the encoders accepts a presentation time stamp (PTS) from the controller 216. The PTS is a wrap-around binary time stamp that is used to assure that the video information is properly synchronized with the audio information after encoding and decoding. A PTS time stamp is sent with each I-frame of the MPEG encoded data.

In one embodiment of the present invention, each encoder 202 is a second generation Motion Picture Experts Group (MPEG-2) encoder, but other decoders implementing other coding techniques can be used as well. The data channel can be subjected to a similar compression scheme by an encoder (not shown), but such compression is usually either unnecessary, or performed by computer programs in the computer data source (for example, photographic data is typically compressed into *.TIF files or *.JPG files before transmission). After encoding by the encoders 202, the signals are converted into data packets by a packetizer 204A-204F (collectively referred to hereinafter as packetizer(s) 204) associated with each source 200, 206-210.

The data packets are assembled using a reference from the system clock 214 (SCR), a control word (CW) generated by the conditional access manager 208, and a

system channel identifier (SCID) generator 210 that associates each of the data packets that are broadcast to the subscriber with a program channel. This information is transmitted to the packetizers 204 for use in generating the data packets. These data packets are then multiplexed into serial data, encoded, modulated, and transmitted. A special packet known as a control word packet (CWP) which comprises control data including the control word (CW) and other control data used in support of providing conditional access to the program material is also encrypted and transmitted.

FIG. 3A is a diagram of a representative data stream. The first packet segment 302 comprises information from video channel 1 (data coming from, for example, the first video program source 200A). The next packet segment 304 comprises computer data information that was obtained, for example from the computer data source 206. The next packet segment 306 comprises information from video channel 5 (from one of the video program sources 200), and the next packet segment includes information from video channel 1 (again, coming from the first video program source 200A). The data stream therefore comprises a series of packets from any one of the data sources in an order determined by the controller 216. The data stream is encrypted by the encryption module 218, modulated by the modulator 220 (typically using a QPSK modulation scheme), and provided to the transmitter 222, which broadcasts the modulated data stream on a frequency bandwidth to the satellite via the antenna 106.

Subscribers 110 receive media programs via a subscriber receiver or IRD 132. Using the SCID, the IRD 132 reassembles the packets to regenerate the program material for each of the channels. As shown in FIG. 3A, null packets created by the null packet module 312 may be inserted into the data stream as desired.

FIG. 3B is a diagram of a data packet. Each data packet (e.g. 302-316) is 147 bytes long, and comprises a number of packet segments. The first packet segment 320 comprises two bytes of information containing the SCID and flags. The SCID is a unique 12-bit number that uniquely identifies the data packet's data channel. The flags include 4 bits that are used to control whether the packet is encrypted, and what key must be used to decrypt the packet. The second packet segment 322 is made up of a 4-bit packet type indicator and a 4-bit continuity counter. The packet type identifies the packet as one of the four data types (video, audio, data, or null). When combined with the SCID, the

packet type determines how the data packet will be used. The continuity counter increments once for each packet type and SCID. The next packet segment 324 comprises 127 bytes of payload data, which is a portion of the video program provided by the video program source 200. The final packet segment 326 is data required to perform forward
5 error correction.

ENCRYPTION OF MEDIA PROGRAMS

Media programs are encrypted by the encryption module 218 before transmission to assure that they are received and viewed only by authorized subscribers. Each media
10 program is encrypted according to an alphanumeric encryption key referred to hereinafter as a control word (CW). This can be accomplished by a variety of data encryption techniques, including the data encryption standard (DES) and the Rivest-Shamir-Adleman (RSA) algorithm.

To decrypt the media programs, the subscriber's 110 IRD 132 must also have
15 access to the CW. To maintain security, CWs are not transmitted to the IRD 132 plaintext. Instead, CWs are encrypted before transmission to the subscriber's IRD 132. The encrypted CW is transmitted to the subscriber's IRD 132 in a control word (data) packet.

In one embodiment, the data in the CWP, including the CW, is encrypted and
20 decrypted via what is referred to hereinafter as an input/output (I/O) indecipherable algorithm.

An I/O indecipherable algorithm is an algorithm that is applied to an input data stream to produce an output data stream. Although the input data stream uniquely determines the output data stream, the algorithm selected is such that it's characteristics
25 cannot be deciphered from a comparison of even a large number of input and output data streams. The security of this algorithm can be further increased by adding additional functional elements which are non-stationary (that is, they change as a function of time). When such an algorithm is provided with identical input streams, the output stream provided at a given point in time may be different than the output stream provided at
30 another time.

So long as the encryption module 218 and the IRD 132 share the same I/O indecipherable algorithm, the IRD 132 can decode the information in the CWP to retrieve the CW. Then, using the CW, the IRD 132 can decrypt the media program so that it can be presented to the subscriber 110.

5 To further discourage piracy, the control data needed to decrypt and assemble data packets into viewable media programs may be time-varying (the validity of the control data in a CWP to decode a particular media program changes with time). This can be implemented in a variety of ways.

10 For example, since each CWP is associated with a SCID for each media program, the SCID related to each CWP could change over time.

15 Another way to implement time-varying control data is to associate time stamps with the received data stream and the CWP control data. In this case, successful decoding of the CWP to produce the CW would require the proper relationship between the time stamps for the data stream and the control data in the CWP. This relationship can be defined, for example, by changing the decryption scheme used to generate the CW from the CWP according to the received time stamp for the data stream. In this case, if the time stamp of the received data stream does not match the expected value, the wrong decryption scheme will be selected and the proper CW (to decrypt the program material) will not be produced. If, however, the time stamp of the received data stream matches the
20 expected value, the proper decryption scheme will be selected, and the CWP decryption scheme will yield the proper CW.

REQUESTING PAY-PER-VIEW SERVICES

25 The data required to receive pay-per-view (PPV) media programs are stored in the CWP and in another data packet known as the purchase information parcel (PIP). Both the CWP and the PIP are broadcast to the subscriber via the video distribution system 100 in real time. As described below, the CWP is used by the IRD 132 to retrieve PPV media programs.

30 Generally, PPV services can include operator-assisted pay-per-view (OPPV) and impulse pay-per-view (IPPV) services. When requesting OPPV services, the subscriber 110 must decide in advance that they desire access to a particular media program. The

subscriber 110 then calls an entity such as the control center 102, and requests access to the media program. When requesting impulse pay-per-view services (IPPV), the subscriber 110, while viewing the program guide, moves the cursor over the viewer channel associated with the desired media program, and selects "enter." After the
5 decision and rights to purchase a PPV program are confirmed (for example, by checking channel lockouts, rating limits, and purchase limits), a purchase information parcel (PIP) is received and stored in the subscriber's conditional access module 406 (which is described in more detail below) for further use. The conditional access module 406 associates the information in the CWP and the PIP, and uses the PIP in conjunction with
10 the CWP to verify that the subscriber 110 should be provided access to the media program and to decrypt the media program.

Ordering PPV media programs in advance using the PIP is limited, however, since the PIP is broadcast up to 24 hours before the media program itself is broadcast. Since the PIP is broadcast in real time, the IRD 132 does not acquire the PIP until the subscriber
15 110 actually requests the PPV media program purchase.

SUBSCRIBER RECEPTION AND DECRYPTION OF MEDIA PROGRAMS

FIG. 4 is a simplified block diagram of an IRD 132. The IRD 132 receives and decrypts the media programs broadcast by the video distribution system 100. These
20 media programs are streamed to the IRD 132 in real time, and may include, for example, video, audio, or data services.

The IRD 132 is communicatively coupleable to a conditional access module (CAM) 406. The CAM 406 is typically implemented in a smart card or similar device, which is provided to the subscriber 110 to be inserted into the IRD 132. The CAM 406
25 interfaces with a conditional access verifier (CAV) 408 which performs at least some of the functions necessary to verify that the subscriber 110 is entitled to access the media programs. The CAV 408 is communicatively coupled to a metadata analysis module (MAM) 411. Using the information in metadata table (e.g. Table 1 described below), the MAM 411 acts as a gate-keeper to determine whether stored media programs will be
30 decrypted and presented to the subscriber 110. This is accomplished by comparing the metadata values with measured or accumulated values. The CAV 408 and the MAM 411

can be implemented as separate modules from the transport/demux/decryptor 412 and the microcontroller and memory 414 as shown, or may be implemented via software instructions stored in the memory and performed by the microcontroller 414.

5 The IRD 132 comprises a tuner 410, a transport and demultiplexing module (TDM) 412, which operates under control of a microcontroller and associated memory 414, a source decoder 416 and communicatively coupled random access memory (RAM) 418, and a user I/O device for accepting subscriber 110 commands and for providing output information to the subscriber.

10 The tuner receives the data packets from the video distribution system and provides the packets to the TDM 412. Using the SCIDs associated with each media program, the TDM 412 reassembles the data packets according to the channel selected by the subscriber 110, and unencrypts the media programs using the CW key. The TDM 412 can be implemented by a single secure chip, and is communicatively coupled to a microcontroller and memory 414.

15 Once the media programs are unencrypted, they are provided to the source decoder 416 which decodes the media program data according to MPEG or JPEG standards as appropriate. The decoded media program is then provided to a D/A converter (if necessary) and provided to external interfaces 404 which can include a media program presentation device such as a television, an audio system, or a computer.
20 The source decoder 416 makes use of communicatively coupled RAM 418 to perform these functions.

The CW key is obtained from the CWP using the CAV 408 and the CAM 406. The TDM 412 provides the CWP to the CAM 406 via the CAV 408. The CAM 406 uses the I/O indecipherable algorithm to generate the CW, which is provided back to the TDM
25 412. The TDM 412 uses the CW to decrypt the media programs. In most IRDs 132, the CAV 408 and the CAM 406 are capable of decrypting one video/audio/data media program at a time.

As described above, to discourage potential pirates, the control data in the CWP used to decode a particular media program may change with time so that it only produces
30 the proper CW when applied to a media program having the proper time stamp. In this case, the CAM 406 can select and/or control the decryption scheme (e.g. the I/O

indecipherable algorithm) according to the time stamp associated with the data stream carrying the media program. If the media program is sufficiently disassociated in time, the improper decryption scheme will be used, and the proper CW to decode the media program will not be produced.

5 Further details regarding the encryption and decryption of media programs can be found in co-pending and commonly assigned U.S. Patent Application Serial No. 09/491,959.

STORAGE AND RETRIEVAL OF MEDIA PROGRAMS IN ENCRYPTED FORM

10 FIG. 5 is a diagram presenting exemplary method steps used to practice one embodiment of the present invention. A data stream is provided by the subscriber antenna 112 and received by the tuner 410 and the TDM 412, as shown in block 502. The data stream includes a plurality of data packets including data packets with the program material 503 encrypted according to a first encryption key (CW key 509), and access
15 control information which is contained within one or more control word packets (CWP) 504. The CWPs 504 include an encrypted version of the CW key 509. The data stream may also include metadata describing information including rights associated with the program material (which may include, for example, replay rights and/or copy rights). These rights include parameters necessary for controlling the replay of program material,
20 including IPPV or pay-per-play services.

The encrypted program material 503 (denoted Encrypted V/A/D in FIG. 5 to indicate that the program material can include video, audio, or other data) is provided to a broadcast decryption module 510. The broadcast decryption module 510 decrypts the encrypted program material according to the CW key 509.

25 The CWPs 504 are provided to a pre-buy module 506 in the CAM 406. The pre-buy module 506 accepts the metadata in the CWP 504 and generates replay and/or copy right data that is used when the subscriber 110 later decides to replay the program material. This replay right data is provided to a communicatively coupled IPPV control module 538 (IPPV CM), which uses this information as well as to purchase (or buy)
30 information provided by the subscriber 110 to determine whether the stored program material should be played back. The IPPV CM module 538 is also communicatively

coupled to a purchase history module 540 (PHM), which collects information required to bill the subscriber 110 for program material that is viewed by the subscriber 110.

The IPPV CM 538 also provides information used to determine whether the program material received by the tuner/TDM 410, 412 is recorded in the media storage device 528. In one embodiment, this information can be obtained from the data stream broadcast by the provider of the program material.

If the program material is to be stored in the media program device 528, the CWP 504 (which at this point includes temporally-variant control data) is then provided to and decrypted by a CWP decryptor module 508. In one embodiment of the present invention, the CWP 506 is encrypted according to an I/O indecipherable algorithm, and the CWP decryptor module 508 includes the application of the I/O indecipherable algorithm. In another embodiment of the present invention, the CWP 504 is encrypted with a key and a DES or RSA algorithm, and the CWP decryptor module 508 involves the application of the key to reconstruct the encrypted data within the CWP 504. The CWP decrypt module 508 can be invoked for all data streams received by the IRD 132, or can be invoked only for data streams associated with media programs that have been selected for recording by the subscriber 110. The pre-buy module 506 accepts data from the user I/O 420 or from the broadcaster indicating that the subscriber 110 would like to purchase and record a particular media program. If such a purchase (advance or pre-buy) has been requested, the CWP decrypt operations depicted in block 508 commence when the media program is broadcast. In another embodiment of the present invention, the broadcaster determines which programs will be stored on the media storage device 528, and the subscriber 110 need not decide in advance which media programs should be stored for later viewing. For example, the broadcaster may store the ten most popular movies in the media storage device 528, and only bill the subscriber 110 when the subscriber opts to view the media program. In this case, the pre-buy module 506 receives the command to store the media program from the broadcaster and initiates the operations performed by the CWP decrypt module 508.

The CW 509 is provided to the broadcast decrypt module 510, which accepts the encrypted program material 503 to produce the decrypted program material 512. The decrypted program material 512 is provided from the broadcast decryption module 510 to

a communicatively coupled copy protection (CP) storage encryption module 514. The storage encryption module 514 re-encrypts the decrypted program material 512 according to a copy protection (CP) key 516 to produce re-encrypted program material 518. Although the CP key 516 can be generated elsewhere, in the preferred embodiment, the CP key 516 is generated within the CAM 406.

In one embodiment, the CP key 516 is derived using a CP generation module in the CAM 406 or elsewhere in the IRD 132 from the metadata in the data stream that is broadcast to the tuner 410. Depending on the metadata, the CP key 516 may also be time variant with the broadcast program material. In another embodiment, the CP key 516 may be augmented with at least a portion of the metadata before being encrypted with the box key 516 and stored in the media storage device 528 as the encrypted CP key 524 (which itself is a "key"). In this embodiment, when the encrypted CP key 524 is decrypted, the CP key 516 and related metadata are both produced. The metadata can then be used to verify and/or control replay of the program material. The CP key 516 may also be internally generated by the IRD 132 without the metadata.

The CP key 516 is also provided to a key encryption module 522 (KEM) which encrypts the CP key 516 with a conditional access module (CAM) key 520, the value of which is typically unique to each CAM 406. The result of this process is an encrypted copy protection key 524. The re-encrypted program material 518 and the encrypted CP key 524 is then provided to the media storage device 528 for storage. The CAM key 520 could be an internal electronic serial number (ESN) of an integrated circuit implementing some or all of the functions of the CAM 406. The media storage device 528 is typically a hard drive, but may be device with sufficient capacity and access time to support recording and/or playback operations of the data stored therein.

When the subscriber 110 decides to play back the stored media programs, an appropriate user input is provided on the user I/O device 420. The user input may comprise a play command, a fast forward command, a reverse command, a fast play or fast reverse play command, or a pause command. In response to the user input, the IPPV CM 538 determines whether the program material in the media storage device 528 should be presented to the subscriber 110. In one embodiment, the user input comprises buy data, which identifies the subscriber 110, and the requested program material. This buy

data is accepted by a purchase module 550, and compared to the program material rights data obtained from the metadata to determine whether the requested program material should be provided to the subscriber 110. If a determination is made that the program material should be provided, information is transmitted to the purchase history module

5 540. The purchase history module 540 stores information required to bill the subscriber the appropriate amount for the use of the program material. Further, if a determination is made that the program material should be provided, a control module 552 directs the re-encrypted program material 518 and the encrypted CP encryption key 524 to be retrieved from the media storage device 528. The control module 552 may also control when the

10 key decryption module 532 decrypts the CP encryption key 524 to produce the CP key 516.

The CP encryption key 524 is decrypted using the CAM key 520 to produce the CP key 516. This CP key 516 and the re-encrypted program material 518 is provided to the storage decrypt module 534. The storage decrypt module 534 decrypts the further

15 encrypted media program material 518 to produce the program material 503.

After suitable processing (i.e. MPEG and or JPEG decoding, decompression, conversion to an analog signal, etc.), the media program is provided to an external interface 404 device, which may include a presentation device such as a display 536.

One advantage of the present invention is that the data processing required to

20 provide pay-per-play services is resident on the CAM 406. Hence, once the user initiates the purchase of the program material or requests trick play functions, the required processing utilized data replayed from the media storage device 528 and not from live streamed data. Since shuttling back and forth between real time viewing and live streamed data is minimized or eliminated, difficulties with the synchronization of data

25 retrieved from the media storage device 528 are minimized.

In one embodiment of the present invention, the data stream received in IRD 132 further comprises metadata including data to control replay rights and copy protection. This metadata can be encrypted and stored in the media storage device 528 for later decryption and use when a request to view the media program is received. Alternatively,

30 the metadata can be encrypted and broadcast in the data stream in real time for all PPV-

enabled media programs, thus obviating the need for storing the information in the media storage device 528.

As described above, the relationship between the CWP 504 and the encrypted media program may be time-varying. The foregoing embodiment of the present invention, the expiration time associated with the SCIDs for the program material from the CWP 506 may be simply ignored.

Although the foregoing has been described with respect to a plurality of encryption modules (e.g. modules 514 and 522) and decryption modules (e.g. modules 508, 510, 532, and 534), the foregoing can be implemented with single encryption module, a single decryption module, or one or more single encryption/decryption module(s). In one embodiment of the present invention, the operations performed by modules 508, 522, and 532, are performed in a single integrated circuit device in, for example, the CAM 406.

Conclusion

The present invention describes a system and method for recording program material for subsequent replay in which encrypted video/audio/data streams with the program material are decrypted prior to disk storage. The CW key 509 is decoded from the CWP 504 via the CAM 406. This requires new CAM 406 functions to be created to permit pre-buying the IPPV program ahead of time and to store this pre-buy information on the CAM 406 or the disk drive. These new CAM 406 functions can be used to correlate different replay right of a broadcast service to control the amount of the time the broadcast service can be replayed. The new CAM 406 functions also include new replay right data packets that do not have an expiration time relationship with the SCIDs associated with the program material. The play right or replay right for the stored program materials are created so that actual play time and program expiration do not restrict the playback service from the disk drive. This embodiment does not require that the CWP 504 be stored on the disk drive.

In addition to processing the replay right metadata, the CAM 406 handles the generation, encryption, and decryption of the CP key 516 and the CAM key 520. A version of the CP key 516 encrypted by the CAM key 520 is stored on the disk drive.

During playback, the replay metadata is retrieved from the disk (in the form of the encrypted CP key 516) and forwarded to the CAM 406. Alternatively, the replay metadata can be stored and retrieved in the CAM 406 instead of (or in addition to) the hard drive. The CP key 516 is also retrieved from the disk and used to decrypt the re-encrypted program material 518. In one embodiment, the CAM 406 also includes a module to install and restore CP keys 516 and CAM keys 520. Preferably, the CP key 516 and CAM key 520 are generated, stored, and maintained in a tamper-proof device. Even though the CWP 504 is not typically stored in the media storage device 528, new metadata is correlating replay and copy rights to the broadcast stream is stored on the media storage device 528.

During playback, the CAM 406 generates the CP key 516 used to decrypt the data stored on the media storage device 528. With the properties of the encrypted CP key 524 and additional CAM 406 functionality, the CAM 406 decrypts the encrypted CP key 524 using the CAM key 520.

In the present invention, the encryption, decryption, and CP key generation functions are performed outside of the CAM 406. Instead of a unique CAM key 520 stored inside the CAM 406 itself, a unique IRD or box key stored in the IRD 132 could be used. To further enhance security, all of these key generating and encryption/decryption functions could be integrated into the transport chip of the IRD 132. This renders the examination of the functionality of the encrypt/decrypted and key generation features very difficult to accomplish. This helps to ensure the integrity of the system, minimizes the number of the changes to the current CAM 406 architecture, and allows the system to be less reliant on the CAM 406.

The foregoing description of the preferred embodiment of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. It is intended that the scope of the invention be limited not by this detailed description, but rather by the claims appended hereto. The above specification, examples and data provide a complete description of the manufacture and use of the composition of the invention. Since many

embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

CLAIMS

What is Claimed is:

1 1. A method of storing program material for subsequent replay, comprising
2 the steps of:
3 (a) accepting encrypted access control information and the program material
4 encrypted according to a first encryption key, the access control information including a
5 first encryption key and control data;
6 (b) decrypting the received access control information to produce the first
7 encryption key;
8 (c) decrypting the program material using the first encryption key;
9 (d) re-encrypting the program material according to a second encryption key;
10 (e) encrypting the second encryption key according to a third encryption key
11 to produce a fourth encryption key; and
12 (f) providing the re-encrypted program material and the fourth encryption key
13 for storage.

1 2. The method of claim 1, wherein the encrypted access control information
2 further comprises temporally-variant control data, and the method further comprises the
3 steps of:
4 decrypting the received access control information to produce the temporally-
5 variant control data; and
6 modifying the temporally variant control data to generate temporally-invariant
7 control data.

1 3. The method of claim 1, wherein steps (b) and (e) are performed in a
2 conditional access module.

1 4. The method of claim 3, wherein the conditional access module is
2 implemented on a smartcard communicatively coupleable to a tuner and a media storage
3 device.

1 5. The method of claim 1, wherein the access control information further
2 comprises metadata describing at least one right for the program material.

1 6. The method of claim 5, further comprising the step of:
2 generating the second encryption key at least in part from the metadata.

1 7. The method of claim 1, wherein steps (b)-(f) are performed in response to
2 a pre-buy message.

1 8. The method of claim 7, wherein the access control information further
2 comprises metadata describing at least one right for the program material, and the method
3 further comprises the step of:
4 generating replay right data from the metadata.

1 9. The method of claim 8, wherein the replay right data is further generated
2 from pre-buy data.

1 10. The method of claim 1, further comprising the steps of:
2 retrieving the stored re-encrypted program material and the fourth encryption key;
3 decrypting the fourth encryption key using the third encryption key to produce the
4 second encryption key; and
5 decrypting the re-encrypted material using the second encryption key.

1 11. The method of claim 10, wherein the step of decrypting the fourth
2 encryption key using the third encryption key to produce the second encryption key is
3 performed in response to a subscriber request to access the program material.

1 12. The method of claim 11, wherein the access control information further
2 comprises metadata describing at least one right for the program material, the subscriber
3 request to access the program material comprises buy data, and the method further
4 comprises the steps of:
5 generating replay right data from the metadata;
6 accepting the buy data;
7 comparing the buy data with the replay right data; and
8 decrypting the fourth encryption key using the third encryption key to produce the
9 second encryption key according to the comparison between the buy data and the replay
10 right data.

1 13. The method of claim 12, wherein steps (b)-(f) are performed in response to
2 a pre-buy message, and wherein:
3 the second encryption key and the third encryption key are stored in a smartcard,
4 and the replay right data is generated from the metadata and the pre-buy message in the
5 smartcard; and
6 the steps of accepting the buy data, comparing the buy data with the replay right
7 data, and decrypting the fourth encryption key using the third encryption key to produce
8 the second encryption key according to the comparison between the buy data and the
9 replay right data are performed in the smartcard.

1 14. The method of claim 1, wherein the re-encrypted program material and the
2 fourth encryption key are stored on a media storage device.

1 15. The method of claim 1, wherein the control data is temporally-variant.

1 16. The method of claim 15, wherein the temporally-variant control data
2 associates an expiration time with the program material.

1 17. An apparatus for storing program material encrypted according to a first
2 encryption key for replay, comprising:
3 a conditional access module, for accepting encrypted access control information
4 including the first encryption key and temporally-variant control data, the control access
5 module comprising:
6 a first decryption module, for decrypting the access control information to
7 produce the first encryption key;
8 a first encryption module, for encrypting a second encryption key with a
9 third encryption key to produce a fourth encryption key; and
10 a second decryption module for decrypting the fourth encryption key to
11 produce the second encryption key.

1 18. The apparatus of claim 17, further comprising:
2 a tuner, communicatively coupleable to the conditional access module for
3 receiving the encrypted access control information and the program material encrypted
4 according to a first encryption key;
5 a third decryption module, for decrypting the program material using the first
6 encryption key produced by the conditional access module;
7 a second encryption module, for re-encrypting the decrypted program material
8 according to the second encryption key; and
9 a fourth decryption module, for decrypting the re-encrypted program material
10 according to the second encryption key.

1 19. The apparatus of claim 18, wherein the conditional access module further
2 comprises:

3 a pre-buy module, for controlling the first decryption module.

1 20. The apparatus of claim 18, wherein the access control information further
2 comprises metadata describing at least one right for the program material.

1 21. The apparatus of claim 20, wherein pre-buy module generates replay right
2 data from the metadata.

1 22. The apparatus of claim 21, further comprising a buy module,
2 communicatively coupled to the pre-buy module.

1 23. The apparatus of claim 22, wherein the buy module comprises:
2 a purchase module for accepting buy data and comparing the buy data and the
3 replay right data from the pre-buy module; and
4 a control module for controlling the second decryption module based on the
5 comparison between the buy data and the replay right data.

1 24. The apparatus of claim 23, further comprising a billing module, for
2 recording the buy data.

1 25. The apparatus of claim 18, wherein the second encryption key is stored in
2 the conditional access module.

1 26. The apparatus of claim 18, wherein the third encryption key is stored in
2 the conditional access module.

1 27. The apparatus of claim 17, wherein the conditional access module is
2 releaseably communicative coupleable to:
3 a tuner for receiving the encrypted access control information and the program
4 material encrypted according to a first encryption key;
5 a third decryption module, for decrypting the program material using the first
6 encryption key from the conditional access module
7 a second encryption module, for re-encrypting the decrypted program material
8 according to the key; and
9 a media storage device.

1 28. An apparatus for storing program material for replay, comprising:
2 means for accepting encrypted access control information and the program
3 material encrypted according to a first encryption key, the access control information
4 including a first encryption key and control data;
5 means for decrypting the received access control information to produce the first
6 encryption key;
7 means for decrypting the program material using the first encryption key;
8 means for re-encrypting the program material using according to a second
9 encryption key;
10 means for encrypting the second encryption key according to a third encryption
11 key to produce a fourth encryption key; and
12 means for providing the re-encrypted program material and a fourth encryption
13 key for storage.

1 29. The apparatus of claim 28, wherein the encrypted access control
2 information further comprises temporally-variant control data, and the apparatus further
3 comprises:

4 means for decrypting the received access control information to produce the
5 temporally-variant control data; and

6 means for modifying the temporally variant control data to generate temporally-
7 invariant control data.

1 30. The apparatus of claim 28, wherein the means for decrypting the received
2 access control information to produce the first encryption key and the means for
3 encrypting the second encryption key according to a third encryption key to produce a
4 fourth encryption key are implemented in a conditional access module.

1 31. The apparatus of claim 30, wherein the conditional access module is
2 implemented on a smartcard communicatively coupleable to a tuner and a media storage
3 device.

1 32. The apparatus of claim 28, wherein the access control information further
2 comprises metadata describing at least one right for the program material.

1 33. The apparatus of claim 32, further comprising:
2 means for generating the second encryption key at least in part from the metadata.

1 34. The apparatus of claim 32, further comprising:
2 means for generating replay right data from the metadata.

1 35. The apparatus of claim 34, wherein the means for generating the replay
2 right data further generates replay right data from pre-buy data.

1 36. The apparatus of claim 30, further comprising:
2 means for retrieving the stored re-encrypted program material and the fourth
3 encryption key;
4 means for decrypting the fourth encryption key using the third encryption key to
5 produce the second encryption key; and
6 means for decrypting the re-encrypted material using the second encryption key.

1 37. The apparatus of claim 36, wherein the means for decrypting the fourth
2 encryption key using the third encryption key to produce the second encryption key is
3 performed in response to a subscriber request to access the program material.

1 38. The apparatus of claim 37, wherein the access control information further
2 comprises metadata describing at least one right for the program material, the subscriber
3 request to access the program material comprises buy data, and the apparatus further
4 comprises:
5 means for generating replay right data from the metadata;
6 means for accepting the buy data;
7 means for comparing the buy data with the replay right data; and
8 means for decrypting the fourth encryption key using the third encryption key to
9 produce the second encryption key according to the comparison between the buy data and
10 the replay right data.

1 39. The apparatus of claim 38, wherein:
2 the second encryption key and the third encryption key are stored in a smartcard,
3 and the replay right data is generated from the metadata and the pre-buy message in the
4 smartcard; and
5 the means for accepting the buy data, means for comparing the buy data with the
6 replay right data, and means for decrypting the fourth encryption key using the third
7 encryption key to produce the second encryption key according to the comparison
8 between the buy data and the replay right data is implemented in the smartcard.

SUPER ENCRYPTED STORAGE AND RETRIEVAL OF MEDIA PROGRAMS WITH
SMARTCARD GENERATED KEYS

ABSTRACT OF THE DISCLOSURE

5 A method and apparatus for storing and retrieving program material for
subsequent replay is disclosed. In summary, the present invention describes a system and
method for storing and retrieving program material for subsequent replay. The method
comprises the steps of accepting encrypted access control information and the program
material encrypted according to a first encryption key, the access control information
10 including a first encryption key and control data; decrypting the received access control
information to produce the first encryption key; decrypting the program material using
the first encryption key; re-encrypting the program material using according to a second
encryption key; encrypting the second encryption key according to a third encryption key
to produce a fourth encryption key; and providing the re-encrypted program material and
15 a fourth encryption key for storage. The apparatus comprises a conditional access
module, for accepting encrypted access control information and the program material
encrypted according to a first encryption key, the encrypted access control information
including the first encryption key and temporally-variant control data, the control access
module comprising a first decryption module, for decrypting the access control
20 information to produce the first encryption key; a first encryption module, for encrypting
a second encryption key with a third encryption key to produce a fourth encryption key;
and a second decryption module for decrypting the fourth encryption key to produce the
second encryption key.

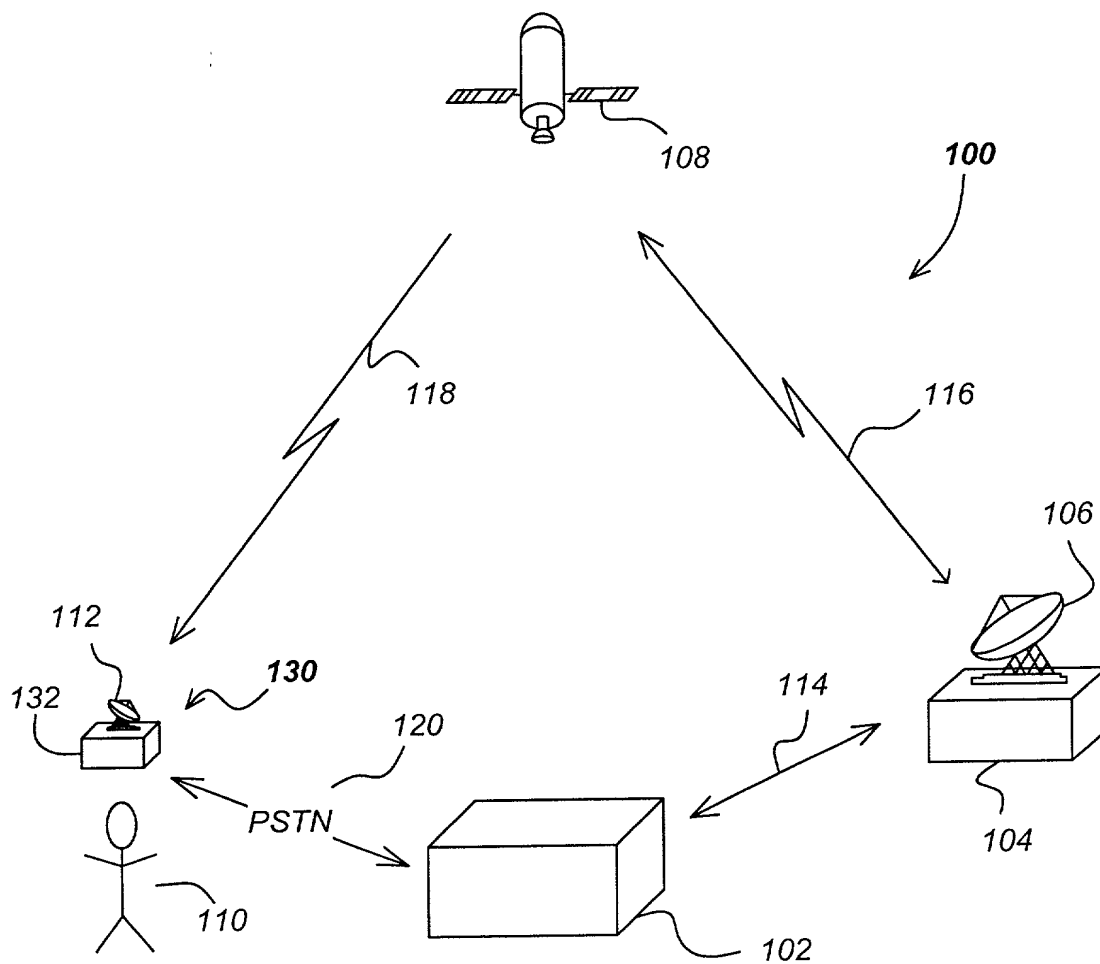
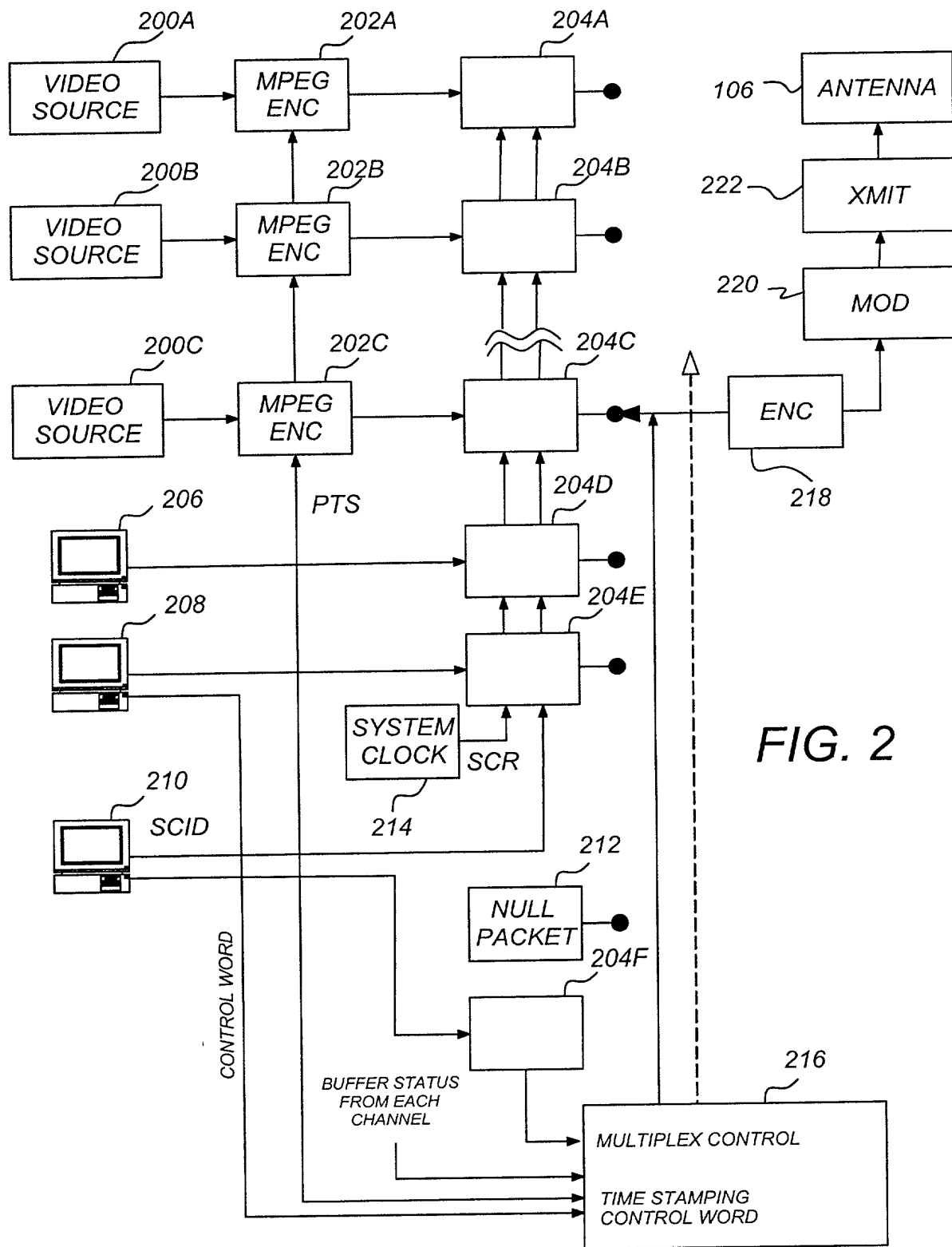


FIG. 1



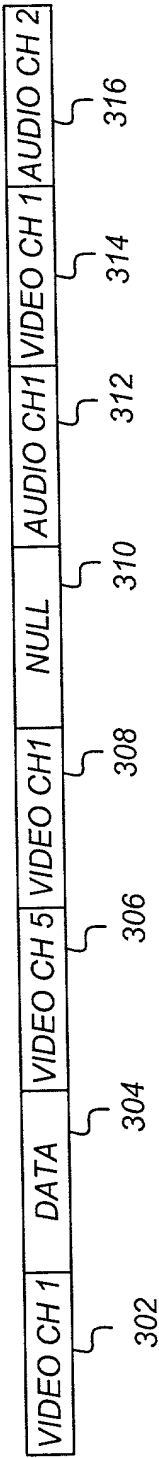
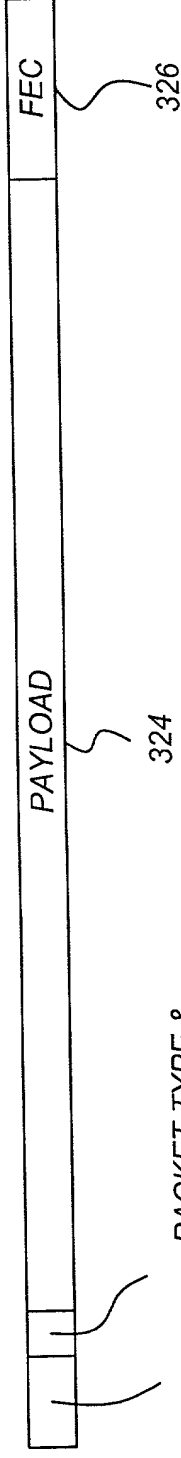
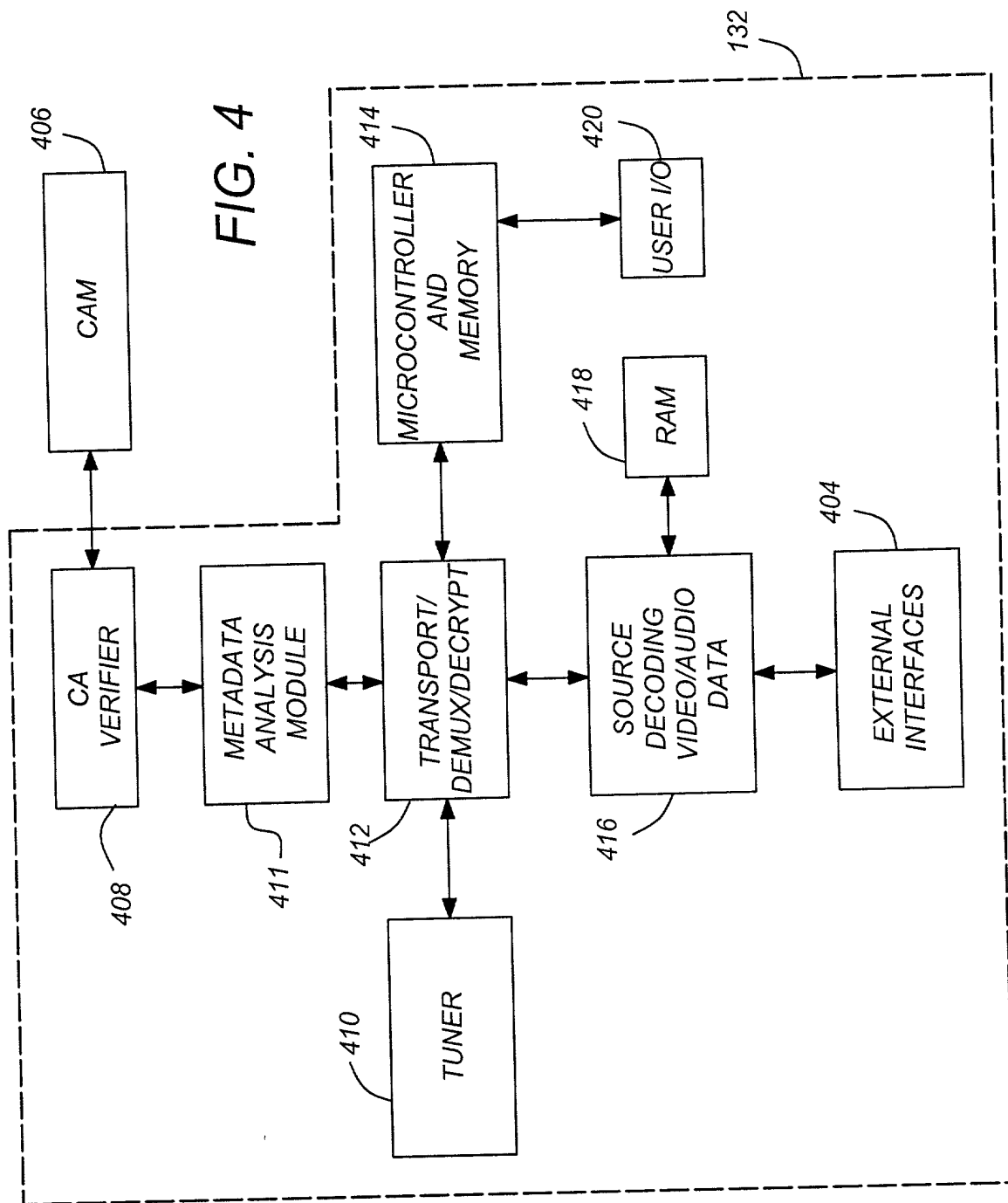


FIG. 3A



SCID & FLAGS 320
PACKET TYPE & CONTINUITY COUNTER 322

FIG. 3B



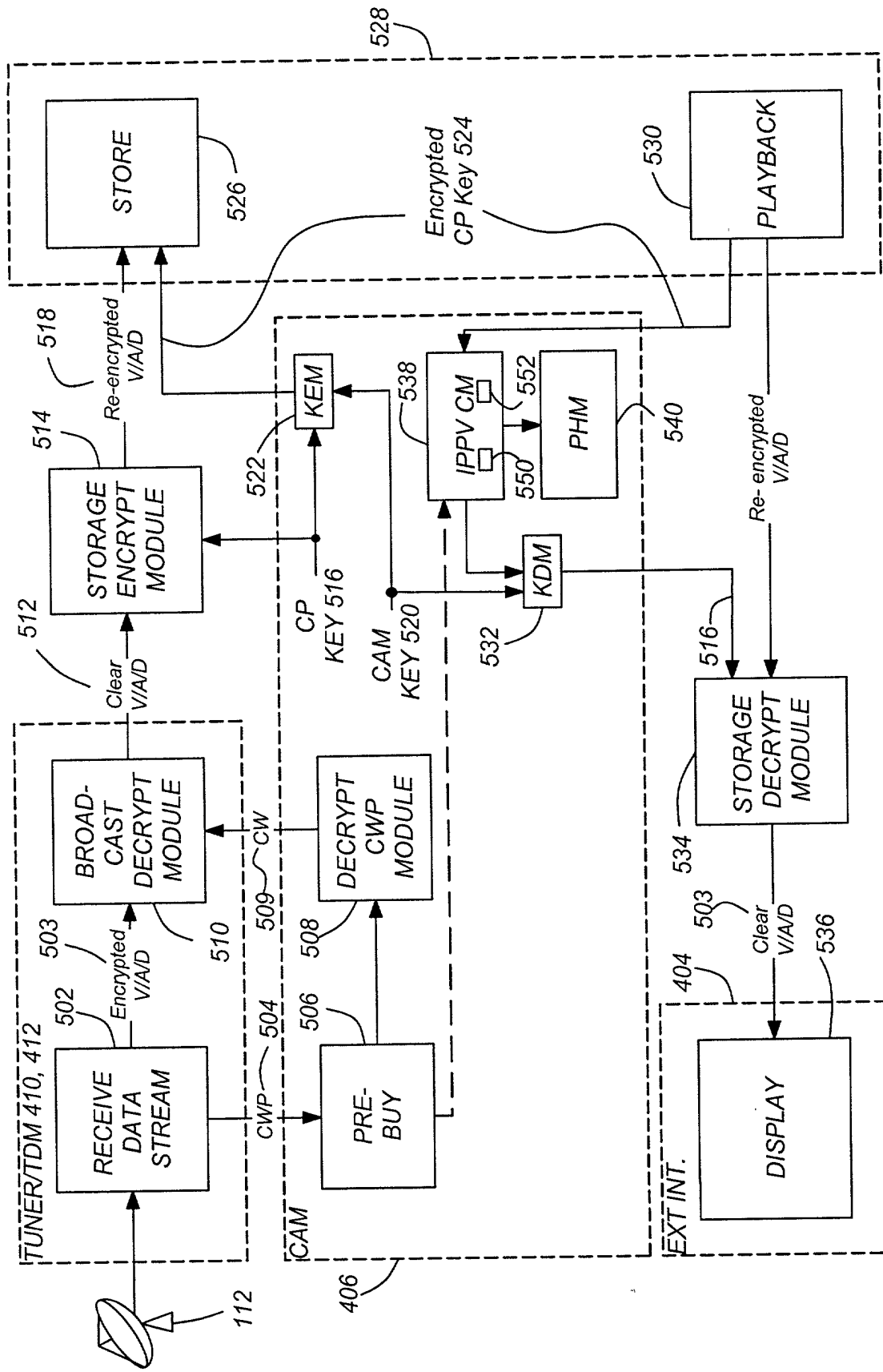


FIG. 5